NUI Galway
OÉ Gaillimh

Semester II Examinations 2011/ 2012

Exam Code(s)	4IF1
Exam(s)	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	
Repeat Paper	No
Discipline(s)	Information Technology
Course Co-ordinator(s)	
Internal Examiner(s)	Professor G Lyons Dr. M Madden Dr C Mulvihill*
External Examiner(s)	Professor M. O'Boyle
No. of Pages	3
Duration	**3 hours**
Instructions:	Attempt any four questions. All questions will be marked equally.

Requirements:
MCQ
Handout
Statistical/ Log Tables
Cambridge Tables
Graph Paper
Log Graph Paper
Other Materials

Release to Library: Yes

PTO

1

(a) Describe the process of capturing information from a suspect PC using the headings (1) sanitizing the forensic disk (2) imaging the suspect disk (3) hashing (4) disk analysis (8 marks)

(b) Discuss the importance of trustworthy (received:) headers in email (6 marks)

(c) A suspect disk contains a scrubbing program. In your opinion does this mean that all hope of recovering any data whatsoever is gone? (6 marks)

2

(a) Give any five properties that a hash function should satisfy (6 marks)

(b) Outline the number theory that underlies an RSA asymmetric encryption scheme, explaining what is meant by Euler's totient (or Phi) function in the course of your discussion (8 marks)

(c) Sketch how a period-finding routine might be used by a quantum computer to defeat an RSA scheme (6 marks)

3

(a) Give your understanding of Public Key Infrastructure using the headings (1) Registration Authority (2) Certification Authority (3) Certificate Revocation List and OCSP (4) Digital Signature (8 marks)

(b) There is a suggestion that your key generation mechanism is not generating sufficiently random material. By considering recent work at EFF and Michigan, or otherwise, discuss the implications of this situation. (6 marks)

(c) Tom has hashed a file for 'authentication purposes' and then encrypted this file with Mary's public key for 'confidentiality purposes'. Tom believes that he can still decrypt this message. Advise on this particular use of hashes and keys. (6 marks)

4

(a) Discuss any three areas that you would expect to be addressed in a typical corporate security policy document for an SME. (6 marks)

(b) Your company has decided to implement a Chinese Wall policy. Explain what this policy means. (6 marks)

(c) You are to review security policy in two environments. In the first, information leakage is considered the biggest risk; in the second untrustworthy information has been identified as a high risk factor. In which environment would you expect that (1) a no write down policy and (2) a no write up policy would be in place? (8 marks)

PTO

5

(a) Explain what is meant by the terms (1) Confidentiality (2) Integrity and (3) Availability (6 marks)

(b) Your company has decided to mandate whole-disk encryption. Give one argument in favour of and one argument against this decision. (8 marks)

(c) What do you understand by the terms 'Annual Loss Expectancy' and 'Acceptable Loss'? Consider a formal risk analysis that produces a prioritised table of identified risks. Do you agree that mitigation measures that have a low cost and high impact should appear towards the top of this table? (6 marks)

6

(a) Solid State Drive technology poses problems for current forensic practice – do you agree? (8 marks)

(b) A suspect claims that they cannot remember the password for an encrypted document. What options are available to you as an investigator? (6 marks)

(c) You are tasked with explaining to bank staff how a phishing attack works. Briefly outline the main points that you would expect to make in connection. (6 marks)

7

"Personal information is increasingly available to interested parties through things like social networking sites and smartphone-resident information mined by downloaded apps." Discuss this statement. (20 marks)